



北京大学
Peking University

Min FENG

MOBILE: (86)1381-000-0050

PHONE: (8610)5896-3453

SEX: Male

DATE OF BIRTH: 06/11/79

PLACE OF BIRTH: Chengdu, Sichuan

EMAIL: minfeng@microsoft.com

ADDRESS:

5F, Beijing Sigma Center, NO. 49, Zhichun Road,

Haidian District, Beijing, P. R. China

Working Experience

✧ July, 2006□Now

Security Team, Internet Multimedia Group, Microsoft Research Asia, Beijing

Post Doc. Associate Researcher

Research on Web Security

- To design an infrastructure for websites' secure mash-up. (Mashup Security)
 - a) Develop technologies to mashup several web services together without security issues.
 - b) Enable cross domains' communication and resist cross domain web attack.
 - c) We built a "process" concept and object orientated concept for frames of web pages. Properties, Methods, Events are exposed to other web pages by clear saying of the container.
- Designed technologies to enhance and convenient web login. (Secure Web Login)
 - a) Users' password is enhanced without losing convenience.
 - b) Design secure login protocols for secure web login with a mouse or a handheld, which supported mutual authentication, anti-phishing, two factors authentication, etc.
 - c) Developed the demos, which are shown on Techfest and Science Fair conferences.
- To design and develop an infrastructure for transactions at anywhere, with any devices, in anytime. (Transaction)
 - a) Sale-Sense: Every web page becomes a front store. People can buy things while surfing a web.
 - b) Develop technologies to enable offline transactions without online trusted third party.
 - c) Social network based distribution and viral marketing.

Research on DRM systems

- Virtual Theater
 - a) Enable buddies to watch movies together while chatting with each other in messenger.
 - b) Introduction theater mode rights to DRM system
 - c) The watching experience is shared by our program, but the content is under protection.
- Designed a novel content encryption key scheme for multicast encryption and DRM.
- Designed a privacy protection scheme for DRM by using partially blind signature.

✧ Aug., 2003□Dec., 2005

Intel China Software Enabling, China Intel Software Center, Shanghai

Intern, Communication Hub for Small & Medium Business

- Developed a system service containing VoIP, fax and email communication methods in C/C++ based on Intel's Architecture.
- Considered security issues of this project and design security solutions.
- Developed demo application for Small & Medium Business. For example: conference call, Interactive Voice Response, SMS, Fax, etc.
- Tested problems with formal test methods and tools, like CPPUNIT.
- Executed the whole cycle of software development from the initial market research and produce specifications to implementation and supporting.

✧ Dec., 2004□Aug., 2005

Cryptography Laboratory, Peking University, Beijing

- In collaborating with Microsoft Research Asia to develop security solutions for portable devices and embedded

systems.

- Designed efficient algorithms for elliptic curve cryptography which can resist power-analysis.
- ✧ Nov., 2004□Jan., 2005 **University of Electronic Science and Technology of China, Chengdu**
Project Leader, Efficient Algorithms for Elliptic Curve Cryptography
 - Collaborated with University of Electronic Science and Technology of China and organized a team to implement efficient ECC algorithms.
 - Played leadership in architecture and algorithm design. Defined C interfaces of all modules, made optimization scheme decision of different layers, etc.
 - Taught the members elliptic curve cryptography theory in a simple way.
 - Be good at algorithm design and analysis, especially about scalar multiplication and multi-precision algorithms.
 - Wrote core algorithms in C and assemble language which was optimized for Pentium instruction sets.
- ✧ Sep., 2002□Apr., 2004 **Cryptography Laboratory, Peking University, Beijing**
Core Member, National Science Fund Project—Elliptic Curve Cryptography over Infinite Number Fields
 - Designed new elliptic curve cryptography over Infinite Number Fields. It fits long data's encryption and has high ratio of point compression. Moreover, I deduced all the theorems strictly.
 - I implemented the whole test program
- ✧ Dec., 2003□Feb., 2004 **Intern, Internet Multimedia Group, Microsoft Research Asia, Beijing**
Research on security issues for portable wireless devices
 - Designed a practical secure portable wireless device include function design and hardware design.
 - Learned smart card architecture.
 - Got familiar with security problems of WAP, UWB, Bluetooth and 802.11 technologies.
- Research on scalable DRM systems
 - Designed a novel scalable layered access control framework for multimedia DRM. The framework solves the key distribution of different access types and multiple access layers.
 - In April and May 2005, we designed an efficient key scheme for multi-type multi-level scalable access.
- ✧ Jun., 2002□Dec., 2003 **Cryptography Laboratory, Peking University, Beijing**
Project Leader, Virtual Private Network (VPN)
 - We made use of Netfilter Technology in Linux and implemented a VPN system which uses our proposed efficient key distribution scheme.
 - I played leadership in architecture design. Did module analysis, framework design, etc.
 - I accumulated much experience of project development. For instance: using CVS for team programming, creating mailing list for easy communication, interface design, mastering document skills and so on.
 - The project integrated several kinds of computer technologies. For example: TCP/IP programming, state machine, compilers principles, multi-thread programming and so on.
 - Be familiar with implementation of network protocols. For instance: we implemented the IPSec/IKE protocols in C.
- ✧ Sep., 2000□Nov., 2000 **Cryptography Laboratory, Peking University, Beijing**
Programmer, RSA algorithm
 - Implemented the RSA algorithm in ASM and C.
- ✧ Sep., 2003□Feb., 2004 **School of Mathematical Science, Peking University, Beijing**
Teaching Assistant, Teaching the Exercise Course of Algebra for our department students
 - My class got the highest average score among four classes in the same final examination.

Patent Applications

- ✧ Bin Zhu, Min Feng, and Shipeng Li, Scalable Layered Access Control For Multimedia, filed with US Patent Office in June 2004.
- ✧ Bin Zhu, Min Feng, and Shipeng Li, Elliptic Curve Point Multiplication, filed with US Patent Office in June, 2005.
- ✧ Bin Zhu, Min Feng, and Shipeng Li, Secure Key Management for Scalable Codestreams, filed with US Patent Office in July, 2005.
- ✧ Min Feng and Bin Zhu, Content Encryption Schema For Integrating Digital Rights Management With Encrypted Multicast, filed with US Patent Office in Jan. 2007

Publications

- ✧ Min FENG, Bin B. ZHU, "A DRM System Protecting Consumer's Privacy", Consumer Communications & Networking Conference (CCNC) 2008, accepted
- ✧ Bin ZHU, Min FENG, Fen LIU, Lei HU "Analysis on AACs' Trallor Tracing against Mix-and-Match Attacks", Consumer Communications & Networking Conference (CCNC) 2008, accepted
- ✧ Jun SHAO, Min FENG, Bin ZHU, Zhenfu CAO, "An Efficient Certified Email Protocol", Information Security Conference 2007
- ✧ Min FENG, Bin B. ZHU, "When DRM Meets Restricted Multicast - A Content Encryption Key Scheme for Multicast Encryption and DRM", Consumer Communications & Networking Conference (CCNC) 2007
- ✧ XU Maozhi, ZHAO Chunlai, FENG Min, REN Zhaorong, YE Jiqing, "Cryptography on Elliptic Curve over p -adic Number Fields", Science in China, April 2004.
- ✧ Min FENG, Bin B. ZHU, Cunlai ZHAO, Shipeng LI, "Signed MSB-Set Comb Method for Elliptic Curve Point Multiplication", Information Security Practice and Experience Conference (ISPEC) 2006, Oct. 2005.
- ✧ Bin B. ZHU, Min FENG, Shipeng LI, "Secure Key Management for Flexible Digital Rights Management of Scalable Codestreams", IEEE Int. Workshop Multimedia Signal Processing 2005
- ✧ Bin B. ZHU, Min FENG, Shipeng LI, "A Framework of scalable Layered Access Control for Multimedia", IEEE Int. Symp. Circuits and Systems 2005, pp. 2703-2706, May 2005.
- ✧ Bin B. ZHU, Min FENG, Shipeng LI, "An Efficient Key Scheme for Layered Access Control of MPEG-4 FGS Video", IEEE Int. Conf. Multimedia & Expo, vol. 1, pp. 443-446, Taiwan, June 2004.
- ✧ FENG Min, ZHAO Yang, Xu Maozhi "A VPN Implementation Scheme based on Netfilter Technology", China Information Security, vol. 2004, no. 10, pp 87-89, 2004.

Education

Sep, 2001□Jul, 2006 PhD School of Mathematical Science, Peking University

Focus on: Cryptography & Network Security

Overall GPA: 3.71/4.0, Major: 3.82/4.0

Sep, 1997□Jul, 2001 B.S. School of Mathematical Science, Peking University

Overall GPA: 3.42/4.0, Major: 3.64/4.0